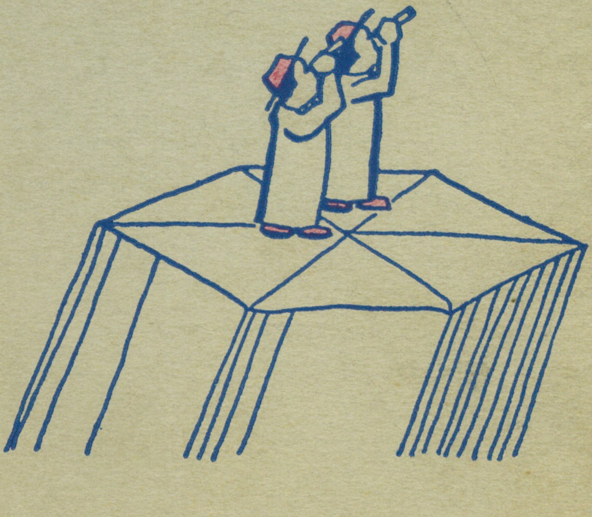
galois and the theory of groups



Given:

a group, G, with n elements in it; and a sub-group, H, containing r elements.

To show that r is a factor of n. Let the elements of H be: $a_1, a_2, a_3, \ldots\ldots\ldots, a_r$.

Now choose some element, b, in G but not in H, and multiply it by each of the r elements in H, obtaining: a_1b, a_2b, a_3b, ..., a_rb; that is, r elements, all distinct from each other and from the elements in H. If $n > 2r$, take another element, c, in G, but not among these 2r elements, and multiply it by the a's; these products must be in G and must be distinct from the 2r elements previously obtained. Thus, each time that the r elements of H are multiplied by an element in G, not previously used, a whole row containing r elements is obtained, until finally all the elements in G

are accounted for:

in other words, the elements in G may be arranged as follows:

$a_1, \quad a_2, \quad a_3, \ldots\ldots a_r;$

$a_1b, \quad a_2b, \quad a_3b, \ldots\ldots a_rb,$

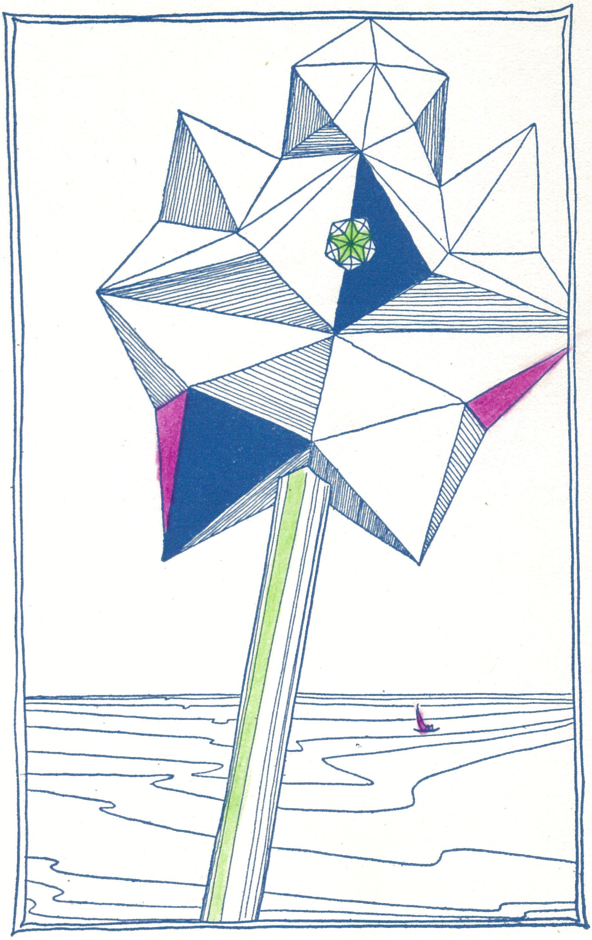
$a_1c, \quad a_2c, \quad a_3c, \ldots\ldots a_rc,$

etc.

And the total number of elements, n, is thus necessarily a multiple of the number of elements in the first row.

That is, r is a factor of n

A

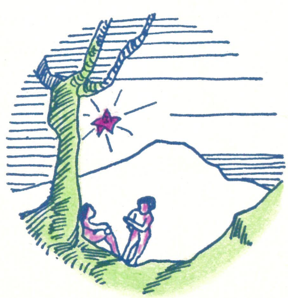


Galois and the Theory of Groups:

A Bright Star in Mathesis.

Text by
Lillian R. Lieber

Drawings by
Hugh Gray Lieber



Second Printing
1941

The Science Press Printing Company
Lancaster, Pennsylvania

PREFACE

This is the second
Of a series
Of little books
On modern mathematics.
The first is on
Non-Euclidean geometry.
The kind of reception which
It received,
Is responsible for the appearance
Of this second one.

INTRODUCTION

It is well-known that
Scientific knowledge
Is increasing all the time,
That science is a
Living, growing subject.

But one generally thinks of
Mathematics as being
So old and so "finished",
That it cannot grow any more.

Indeed
The mathematics
(Arithmetic, algebra, geometry)
Taught in the schools
Was known
CENTURIES AGO;
And even the
Usual COLLEGE course
Dates back
THREE HUNDRED YEARS,
For analytics was created by Descartes
And calculus by Newton,
Both in the 17th century.

And yet the fact is
That mathematics,
EVEN TO A GREATER EXTENT THAN SCIENCE,
Has moved steadily forward
Since that time.

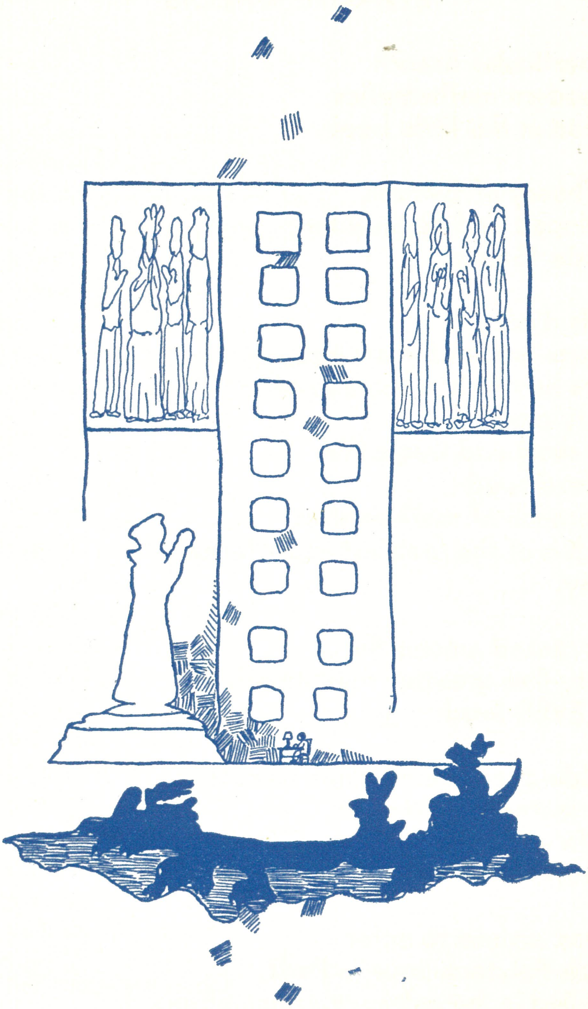
What are some of these
More recent ideas in mathematics?
Are they so abstract
That the young people of this generation
May not even hear them mentioned,
Although many of them were created
By very YOUNG mathematical geniuses?
Are they so hopelessly remote

From ordinary ways of thinking
That the layman may not get
ANY use or pleasure from them?
That even
Most teachers of mathematics
May not have the opportunity
Of becoming acquainted with them?

BY NO MEANS!

The truth is that
These recent developments
In mathematics
Are not only
Of interest to mathematicians,
But are as great a help
To the SCIENTIST
As ever calculus was;
The PHILOSOPHER finds
That modern mathematics
Has a direct bearing
On fundamental ideas
Of the universe.
The PSYCHOLOGIST will see
In modern mathematics
A great instrument
For freeing the mind from prejudices,
And for building
New and powerful structures
Upon the ruins of these old prejudices
(As in the creation of Non-Euclidean geometry).
Indeed EVERYONE can appreciate
The remarkable
ORIGINALITY and FERTILITY
Of modern mathematics.

This little book is intended to serve
As an introduction to one branch of
Modern mathematics,
That it may make further reading on the subject
Easier and pleasanter.



ÉVARISTE GALOIS

The particular branch
Of modern mathematics
Treated in this little book
Is
The Theory of Groups,
Developed and applied by
Évariste Galois.

Galois died,
Just one hundred years ago,
Before he reached the age of
Twenty-one!
In his short and tragic life
He developed
This branch of mathematics,
Which is of the greatest importance
To-day.

He is ranked among the
Twenty-five greatest mathematicians
That EVER lived.[1]

Outside of his tremendous success
In his mathematical work,
His life was a series of
Frustrations.

He was anxious to enter
L'Ecole Polytechnique in Paris,
But failed in the entrance examination;
He tried again a year later,
But was failed again!

---

[1] G. A. Miller in Science, Jan. 22, 1932.

He sent a résumé of his work
To Cauchy and Fourier,
Two outstanding mathematicians
Of that time,
But neither one
Paid any attention to him,
And both lost his manuscripts!

Some of his teachers said of him:
"He knows absolutely nothing."
"He has very little intelligence,
Or else he has so successfully hidden it
That it has been
Impossible for me to discover it."

He was expelled from his school.
He was imprisoned for being
A Revolutionist.

He was "framed"
To fight a duel
In which he was killed.

Peace to his spirit.

On the night before the duel,
Having a presentiment that he would be killed,
He hurriedly wrote out
Some of his mathematical ideas
And sent them to a friend.
(See the biography of Galois
By M. P. Dupuy
In the
Annales de l'Ecole Normale Superieure, 1896.
See also the very interesting
"Source Book in Mathematics"
By David Eugene Smith.)

I. THE IMPORTANCE OF GROUPS.

Before discussing the theory itself,
It will be interesting to give
One of the many reasons
Why it is so important.

It is common knowledge that
One of the important functions
Of mathematics
Is
To solve equations.
Algebraic equations[1] may be classified
According to their degree.
An equation of the
FIRST DEGREE

$$ax + b = 0$$

Can be solved[2]
By any child who has had
A first course in algebra.[3]
The solution here is

$$x = -b/a.$$

---

[1] The term "algebraic equation"
Has a very SPECIFIC meaning.
It means an equation of the form

$$a_0x^n + a_1x^{n-1} + \ldots\ldots\ldots + a_n = 0$$

Where n is a positive integer only.

[2] Except only when $a = 0$ and $b \neq 0$.

[3] Equations of the first degree
Were solved as far back as 1700 B. C.
This is the date of
One of the earliest known mathematical documents,
"Ahmes Papyrus";
It has recently been published
Under the auspices of the
Mathematical Association of America.

The solution of an equation of the
SECOND DEGREE

$$ax^2 + bx + c = 0$$

Is also generally included
In such an elementary course.
The solution is

$$x = (-b \pm \sqrt{b^2 - 4ac})/2a.$$

The ancient Babylonians[1] were able to solve
Equations of this type
Many centuries B.C.

The solution of the
THIRD DEGREE equation

$$ax^3 + bx^2 + cx + d = 0,$$

And that of the
FOURTH DEGREE

$$ax^4 + bx^3 + cx^2 + dx + e = 0,$$

Were much more difficult
Than those of the
First and second degrees
And were not obtained until
The 16th century.
These solutions
May be found in
Any book on the
Theory of Equations.

And so,
As the degree increased,
The solution became
Rapidly more difficult,
And although
Mathematicians could not solve
General equations of degree
HIGHER THAN FOUR

---

1 See the article on
"The Oldest Extant Mathematics"
By G. A. Miller
In "School and Society"
June 18, 1932, p. 833.

Still they[1] believed
That such equations
Could be solved
And eventually would be.
And it was not until
The 19th century
That this was shown,
By means of the
Theory of Groups,
To be
IMPOSSIBLE.

It is important
To make clear at this point
Just what is meant by
"IMPOSSIBLE".

Whether a problem
Can or cannot be solved
Depends upon the
Conditions imposed upon the solution.
Thus,

$$x + 5 = 3$$

CAN be solved IF
Negative numbers are permitted,
But CANNOT be solved IF
Negative numbers are NOT permitted.

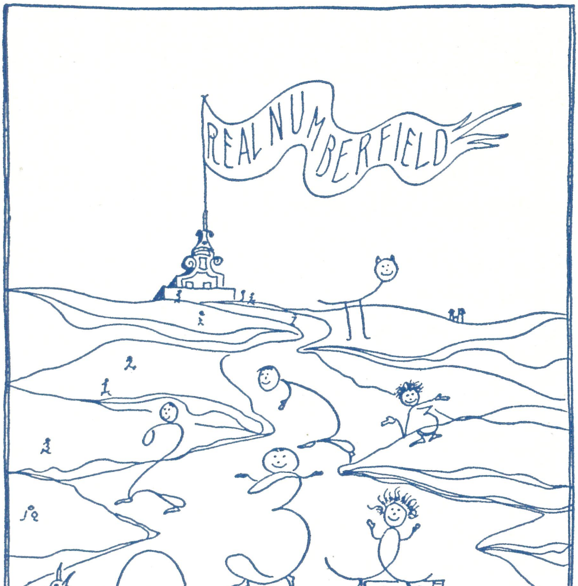
Similarly,

$$2x + 3 = 10$$

CAN be solved IF
X represents a number of dollars,
But CANNOT be solved IF
X represents a number of people,
Since $x = 3\frac{1}{2}$.
An angle CANNOT, in general,

---

[1] Even Euler,
The leading mathematician
Of the 18th century.


REAL NUMBERFIELD

Be trisected
IF RULER AND COMPASSES ONLY
Are to be used,
But CAN be trisected IF
OTHER INSTRUMENTS are permitted.

An algebraic expression may be
REDUCIBLE (that is, FACTORABLE)
Or IRREDUCIBLE (NOT FACTORABLE)
Depending upon the
FIELD[1] in which
The factoring is to be done.
Thus,

$$x^2 + 1$$

Is irreducible in the
Field of REAL numbers,
But REDUCIBLE in the
FIELD OF COMPLEX NUMBERS,
Since the factors of $x^2 + 1$
Are $x + i$ and $x - i$,
Where $i = \sqrt{-1}$.
In other words,
It is meaningless to say

---

[1] A FIELD is a set of numbers
Such that
The sum, difference, product and quotient
(Division by zero being ruled out)
Of any two of them
Are also included in the set.
Thus all complex numbers form a field;
The real numbers alone also form a field;
The rational numbers alone form a field;
But the integers alone do NOT form a field,
Since the QUOTIENT of two integers
Is not necessarily an integer.
A splendid presentation of
Various kinds of interesting "fields"
(Or "realms", as they are sometimes called)
May be found in
"The Theory of Algebraic Numbers"
By L. W. Reid,
A delightful book to read.

That an expression
CAN or CANNOT be factored
Without specifying the FIELD.

Thus mathematicians have learned
The importance of
Specifying the ENVIRONMENT
In which
A statement is TRUE or FALSE
Or perhaps entirely meaningless
And hence NEITHER TRUE NOR FALSE!

Now, then,
In what sense
Has it been proved impossible
To solve the general equation
Of degree higher than four?
The answer is
That it is impossible
To solve it by radicals.
This means that
The unknown CANNOT be expressed
In terms of the coefficients
By the use of
Rational operations
(Namely, addition, subtraction, multiplication and division)

And extraction of roots
ONLY,[1]
A finite number of times.

---

[1] The rational operations
And extraction of roots
Were the only algebraic operations known
At the time when the
Third and fourth degree equations
Were successfully solved,
And therefore
Attempts to solve
Equations of higher degrees
Were limited to these elementary operations.

To illustrate,
In the first degree equation

$$ax + b = 0,$$

We have $x = -b/a$;
That is,
X CAN be found
By dividing (which is a rational operation)
The constant term b
By the coefficient a.
In the second degree equation

$$ax^2 + bx + c = 0$$

We have

$$x = (-b \pm \sqrt{b^2 - 4ac})/2a$$

Which again is found
From the coefficients
By using
ONLY
THE RATIONAL OPERATIONS
AND EXTRACTION OF A ROOT.

Similarly,
In the solution of the general equations
Of the third and fourth degrees,
x is found in terms of the coefficients
By using these operations only,
A finite number of times.
In other words,
They are SOLVABLE BY RADICALS.

But when we come to
Equations of degree higher than four,
This is no longer true.
This refers, of course,
To the GENERAL equation
Of degree higher than four;
Certain SPECIFIC ones
CAN be solved by radicals.

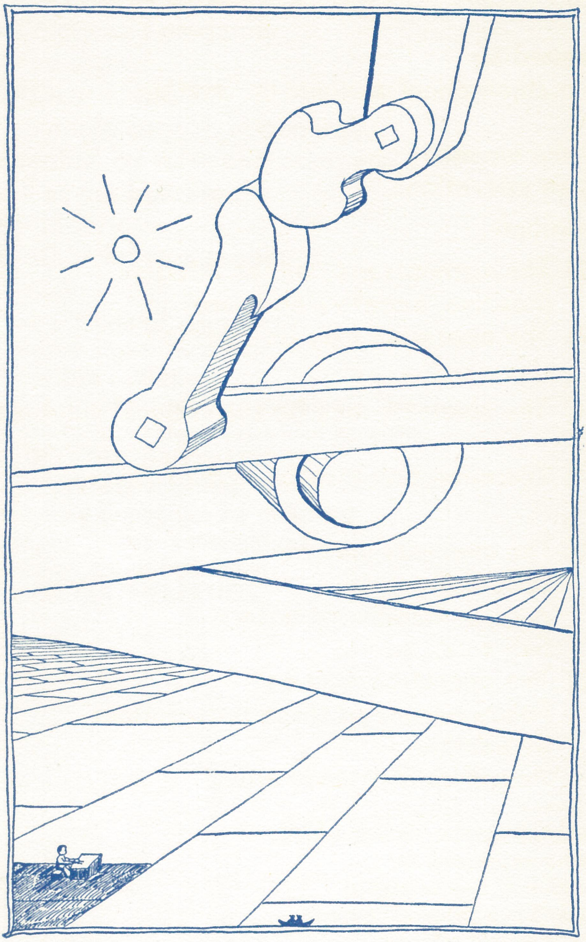
We shall see
How it was proved
By means of GROUP THEORY.

That the GENERAL equation
Of degree higher than four
CANNOT be solved by radicals.[1]

We shall also see
How simply and elegantly
It can be shown
By GROUP THEORY,
That an angle cannot, in general,
Be trisected by ruler and compasses only,
As well as the bearing of
Group theory
Upon other famous problems.

---

[1] For the solution of equations
Of degree higher than four,
Without this limitation,
See L. E. Dickson: Modern Algebraic Theories
And the further references which he gives
(This, of course, does not refer
To approximate solutions,
Which may sometimes be obtained
By graphs, Horner's method, etc.,
And which are of interest in
APPLIED MATHEMATICS.)



II. WHAT IS A GROUP?

The essentials
Of a mathematical machine or "system"
Are
(1) the elements
(2) an operation.

For example,

(a) (1) The elements may be the integers
(Positive, negative and zero)
(2) The operation may be addition.

Or

(b) (1) The elements may be the rational numbers[1]
(except zero)
(2) The operation may be multiplication.

Or

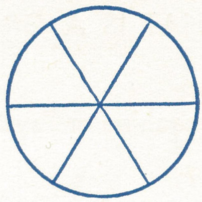
(c) (1) The elements may be
Substitutions of
A given number of letters,
Say x_1, x_2, x_3.
(2) The operation may be
Following one of these substitutions
By another,
As will be illustrated later.

---

[1] A rational number is one which
Can be expressed as
The ratio of two integers:
Thus 3/5 is a rational number,
But $\sqrt{2}$ is not rational,
Since it cannot be expressed
In the form a/b,
Where a and b are integers:
For the proof of this
See p. 23 in
Rietz and Crathorne: College Algebra.

Or

(d) (1) The elements may be
The rotations of the figure:



Through an angle of 60°,
Or multiples of 60°.

(2) And the operation, as in (c),
Following one of these rotations
By another.

And so on,————————.

It might seem
That not much could be done
With so humble a start.
But the power of it
Is amazing,
As will appear soon.

In order that such a system
May be a "Group",
It must have
The following FOUR qualifications:

1. If two elements[1]
Are combined by the given operation
The result must itself be
An element of the system.

For instance,

In (a) above,
If one INTEGER

---

[1] Whether the two elements are distinct
Or the same one taken twice.

Is ADDED to another INTEGER,
The result is an INTEGER.
In (b),
If two RATIONAL NUMBERS
Are MULTIPLIED,
The result is
A RATIONAL NUMBER.

In (c),
If the SUBSTITUTION
x_2 for x_1, x_3 for x_2, x_1 for x_3
Is made in

$$x_1 \; x_2 \; x_3$$

Obtaining

$$x_2 \; x_3 \; x_1$$

And this SUBSTITUTION
FOLLOWED BY
The SUBSTITUTION
x_3 for x_2, x_1 for x_3, x_2 for x_1,
Obtaining

$$x_3 \; x_1 \; x_2$$

The result is
The SUBSTITUTION
x_3 for x_1, x_1 for x_2, x_2 for x_3
In the original given expression.

In (d),
If the ROTATION of the figure
Through 60° (counter-clockwise)
Is FOLLOWED BY
The ROTATION 120° (counter-clockwise)
The result is
The ROTATION 180° (counter-clockwise).

2. The system must contain
The IDENTITY ELEMENT
Which when combined
With any other element
Leaves this other element unchanged.

Thus in (a),
The IDENTITY ELEMENT is
The NUMBER ZERO,
Since
When ZERO is ADDED
To any INTEGER,
It leaves that integer
UNCHANGED.

In (b),
The IDENTITY ELEMENT is
The NUMBER ONE,
Since,
When ONE is MULTIPLIED
By any RATIONAL NUMBER,
It leaves that rational number
UNCHANGED.

In (c),
The IDENTITY ELEMENT is
The SUBSTITUTION
x_1 for x_1, x_2 for x_2, x_3 for x_3,
Since,
When this SUBSTITUTION
Is FOLLOWED BY
Any other SUBSTITUTION,
The result is equivalent to
The latter substitution alone.

In (d),
The IDENTITY ELEMENT is
The ROTATION 360°,
Since,
If this ROTATION
Is FOLLOWED BY
Any other ROTATION in the system,
The result is
That second rotation alone.

3. Each element must have
   An INVERSE ELEMENT,

Such that
If an ELEMENT is
Combined with its INVERSE,
By means of the given OPERATION,
The result is
The IDENTITY ELEMENT.

Thus in (a),
The INVERSE of 3 is —3,
Since 3 ADDED to —3
Gives ZERO.

In (b),
The INVERSE of a/b is b/a,
Since
a/b MULTIPLIED by b/a
Gives 1.

In (c),
The INVERSE of
x_2 for x_1, x_3 for x_2, x_1 for x_3,
Is
x_1 for x_2, x_2 for x_3, x_3 for x_1,
Since,
If one of these SUBSTITUTIONS
Is FOLLOWED BY the other,
The result is
The SUBSTITUTION
x_2 for x_2, x_3 for x_3, x_1 for x_1,
Which is
The IDENTITY SUBSTITUTION.

In (d),
The INVERSE of
A ROTATION of 60° (counter-clockwise)
Is a ROTATION of—60° (clockwise),
Since one of these
FOLLOWED BY the other
Is equivalent to
The IDENTITY ELEMENT.

4. The ASSOCIATIVE LAW must hold.[1]

Since a GROUP[2] must satisfy
These FOUR REQUIREMENTS,
It is obvious that
If ZERO were excluded from (a),
The system would
No longer be a group
Since there would be
No identity element.

Also
The INTEGERS
(Positive, negative and zero)
Would NOT form
A GROUP
Under MULTIPLICATION,
Since
The inverse of 3, for example,
Being 1/3,
Does not exist in this system.

---

[1] This means that
If three elements a, b, and c,
Are given,
And the operation is denoted by o,
Then,
If the associative law holds,
(aob)oc should give
The same result as
ao(boc).
Thus in (a),
$3 + (4 + 5) = (3 + 4) + 5$
Since
$3 + 9 = 7 + 5$.
That is,
The associative law does hold in (a).
It can readily be seen that
It also holds
In (b), (c), and (d) above.

[2] For other simple and interesting
Examples of groups,
See L. C. Mathewson:
Elementary Theory of Finite Groups.

Thus,
Whether or not a system is a group,
Depends upon
THE ELEMENTS IN IT,
THE OPERATION TO BE USED,
And
HOW THESE ELEMENTS BEHAVE
UNDER THIS OPERATION.

It should be noted that:

(1) The elements are
NOT NECESSARILY NUMBERS,
But may be
MOTIONS, as in (d),
Or
ACTS, as in (c),
Etc., Etc.,
Thus widening the
SCOPE OF MATHEMATICS,
By freeing it from
ITS SUBJECTION TO NUMBER ONLY.

(2) The operation is
NOT NECESSARILY
Addition or multiplication,
Or any of the other processes
Which we generally call operations
In arithmetic or algebra,
But may be merely the
Operation of FOLLOWING
(One act by another)
As in (c) and (d).

It is customary,
No matter what the operation,
To
CALL IT "MULTIPLICATION".
Thus we say in (c),
One SUBSTITUTION
IS MULTIPLIED BY another,

Instead of
IS FOLLOWED BY another.
But of course
This use of the word
"MULTIPLICATION"
Should not be confused with
The multiplication
In arithmetic and algebra.
For this more general
MULTIPLICATION
May have
Quite DIFFERENT PROPERTIES
From ordinary multiplication.

For example,
In ordinary multiplication,

$$2 \times 3 = 3 \times 2,$$

And therefore we say that
Multiplication is
COMMUTATIVE,
That is,
The same result is obtained
If the factors are reversed.

But if we
"MULTIPLY", in (c),
One substitution by another,
We may NOT get
The same result
If the two substitutions
Are reversed.
Thus in the expression

$$x_1x_2 + x_3$$

Apply the substitution
x_3 for x_1, x_1 for x_3, and x_2 for x_2,
Which gives

$$x_3x_2 + x_1$$

And "MULTIPLY" IT BY
The substitution

x_2 for x_1, x_3 for x_2, and x_1 for x_3,
Thus obtaining

$$x_1x_3 + x_2$$

As the final result.

If we now reverse the substitutions,
And take the substitution
x_2 for x_1, x_3 for x_2, and x_1 for x_3 first,
We get first

$$x_2x_3 + x_1;$$

Now, "MULTIPLYING" this substitution
By the substitution
x_3 for x_1, x_1 for x_3, and x_2 for x_2,
We get

$$x_2x_1 + x_3$$

As the final result,
Which is
DIFFERENT FROM

$$x_1x_3 + x_2,$$

The final result previously obtained.

Hence,
This kind of
"MULTIPLICATION"
IS NOT COMMUTATIVE.
And it is therefore of
GREAT IMPORTANCE
To indicate
The sequence intended,
And to carry out the operation
In that order.

In the next chapter
We shall indicate
Some interesting facts
In connection with
SUBSTITUTION GROUPS,
For it is this type of group
Which Galois used
In the solution of equations.

But before that,
It would be well to
Show how the
Notation
Can be simplified,
For a simple notation
Is vital
To the progress
Of a subject.[1]

Take for example
The substitution
x_2 for x_1, x_3 for x_2, and x_1 for x_3.
Instead of writing it in this way,
We may omit the x's entirely,
And use only the subscripts,
Thus,

(123).

This means that

1 is changed to 2
2 is changed to 3
And 3 is changed to 1.

In other words,

x_1 is changed to x_2
x_2 is changed to x_3
And x_3 is changed to x_1.

Or, as we said at first,
We substitute
x_2 for x_1, x_3 for x_2, and x_1 for x_3.

Similarly,
x_3 for x_2, x_1 for x_3, and x_2 for x_1,

---

[1] It is easy to understand why
The solution of equations
Did not progress rapidly
So long as the equation was written
In WORDS,
Instead of in SYMBOLS!
(See the "Ahmes Papyrus"
Published under the auspices of
The Mathematical Association of America.)

May be written

(231)

In which, each number
Is changed into
The number that follows it,
And the last number, 1,
Is changed into the first number, 2,
Thus completing the cycle.

In like manner,

(132)

Means the substitution
x_3 for x_1, x_2 for x_3, x_1 for x_2,
And

(13) (2),

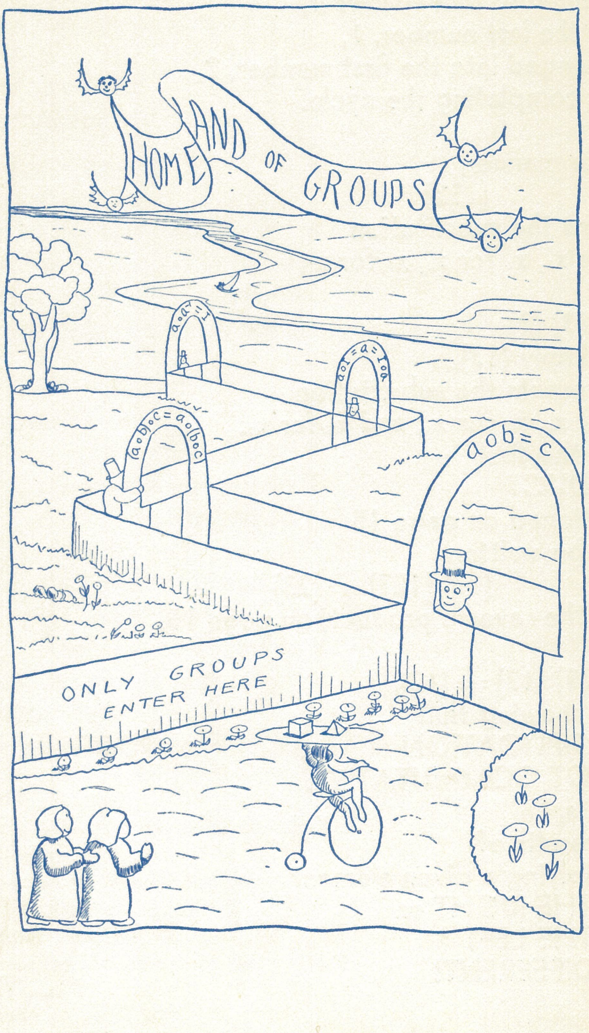
Or simply (13),
Represents the substitution
x_3 for x_1, x_1 for x_3, and x_2 for x_2.
Thus the first
PRODUCT
Mentioned on page 15
Can be written

$$(13)\,(123) = (23)$$

And the reverse product, on page 16,
Is

$$(123)\,(13) = (12),$$

Thus showing that
MULTIPLICATION
IS NOT COMMUTATIVE.
That is,
The results of
Multiplying a given element
ON THE RIGHT or
ON THE LEFT
Are DIFFERENT!



HOMELAND OF GROUPS
$a \circ a^{-1} = I$
$a \circ I = a = I \circ a$
$(a \circ b) \circ c = a \circ (b \circ c)$
$a \circ b = c$
ONLY GROUPS ENTER HERE

III. SOME IMPORTANT FACTS ABOUT GROUPS.

Sometimes it happens that
Some of the elements
Of a group
Form a group among themselves,
Called a
SUB-GROUP.

For example,
Consider the group (a)
In the previous chapter.
If we take
ONLY THE EVEN INTEGERS
(Positive and negative and zero)
And keep addition as the operation,
Then these alone will satisfy
The FOUR REQUIREMENTS
For a group,
Since,

1. The sum of
   Any two EVEN INTEGERS
   Is an EVEN INTEGER.
2. ZERO is the IDENTITY ELEMENT.
3. The INVERSE of
   Any POSITIVE EVEN INTEGER
   Is the
   Corresponding NEGATIVE EVEN INTEGER
   (And vice versa),
   Because
   The sum of two such integers
   Is the identity element,
   ZERO.
4. The associative law holds. (See p. 13.)

Hence,
The EVEN INTEGERS alone
Form a SUB-GROUP
Of the group of ALL integers
Under ADDITION.

Similarly,
A group whose elements are
SUBSTITUTIONS,
That is,
A SUBSTITUTION GROUP,
May also have
A SUB-GROUP.

For example,
Take the six
SUBSTITUTIONS:[1]
I, (12), (123), (132), (13), (23),
Where I represents
The IDENTITY SUBSTITUTION (see p. 11).
These constitute a group,
Since they satisfy
The FOUR requirements,
Namely,

1. The product of any two of them
   Gives a third one of the set,
   Thus,[2] for example,

$$(12)(123) = (13)$$
$$(123)(132) = I$$
$$(13)(23) = (123).$$

Also,
The product of

---

[1] See p. 17 for an explanation
Of the notation.

[2] The result (13) is obtained as follows:
Since in (12), 1 is to be replaced by 2,
And in (123), 2 is to be replaced by 3,
The result is that 1 is replaced by 3.
Further in (12), 2 is to be replaced by 1,
And in (123), 1 is to be replaced by 2,
The result is that 2 remains unchanged.
And finally,
Since in (12), 3 is not mentioned
And therefore not to be changed,
But in (123), 3 is to be changed to 1,
The result is that 3 IS changed to 1.
All these results
Are completely accounted for in (13).

Any one of them by ITSELF
Likewise gives another one of the set,
Thus,

$$(123)\,(123) = (132)$$

And so on for all the rest.

2. There is the identity element, I.
3. Every element has an INVERSE:
   Thus the inverse of (123)
   Is (132),
   Since their product is I.
   Similarly,
   The inverse of (12) is (12),
   And so on.
4. The associative law holds.

Now of these six substitutions (p. 20)
Consider the two, I and (12).
These two alone form a group,
Satisfying the FOUR requirements.
Hence the group consisting of
I and (12)
Is a SUB-GROUP
Of the given group.

It can easily be shown[1] that
The order of any sub-group
(That is, the number of elements in it)
Is a factor
Of the order of the given group.
A very important
Kind of sub-group
Is
An INVARIANT SUB-GROUP.
In order to explain this,
It is necessary first
To explain
What is meant by
The TRANSFORM of

---

[1] See inside front cover.

One element by another.
Take, for example,
The element (12),
And MULTIPLY it
ON THE RIGHT by (123)
And ON THE LEFT by (132).
NOTE THAT (123) and (132) are
INVERSES OF EACH OTHER (see p. 21).
We thus obtain

(132) (12) (123)

Which equals (23).
This result, (23), is called
The TRANSFORM of (12) by (123).

Thus,
If a given element of a group
Is multiplied on the right
By another element,
And on the left
By the inverse of that other element,
The result is called
The TRANSFORM of the given element
By that other element.

Now,
A sub-group is called
INVARIANT
If it remains unchanged[1]
When all of its elements are
TRANSFORMED
By all the elements
Of the original group.

---

[1] Unchanged does NOT necessarily mean
That each element of the sub-group
Remains unchanged,
But that each element becomes
Some element of the sub-group,
So that the sub-group, AS A WHOLE,
Is unchanged.

INVARIANT SUB-GROUPS
Are very important,
As we shall soon see.
Particularly important among them
Is a
MAXIMAL INVARIANT PROPER[1] SUB-GROUP.
It is one which is
NOT CONTAINED in a LARGER
Invariant proper sub-group.

Now if G is a given group,
And if H is a
Maximal invariant proper sub-group of G,
K a maximal invariant proper sub-group of H,
Etc.,
Then if the order of G
(That is, the number of elements in it)
Is divided by the order of H,
And the order of H divided by
The order of K,
Etc.,
The numbers so obtained are called
The COMPOSITION-FACTORS
Of the group G.
And if these are all PRIME NUMBERS,
G is called a SOLVABLE group.[2]
(The significance of the term

---

[1] In general,
A group may be considered
As a sub-group of itself,
But a PROPER sub-group
Is always less than the group itself.
Thus the word "PROPER"
Emphasizes the SUB in SUB-GROUP.

[2] It is important to note that
A group G may, in some cases, be subdivided
Into a series of
Maximal invariant proper sub-groups
IN MORE THAN ONE WAY
(See inside back cover),
But still

"Solvable"
Will appear later.)

Just one more detour:

It sometimes happens that
A group is such
That all of its elements
Are powers of some one element
Other than the Identity.
For example,

Consider the group

$$I, (123), (132).$$

Here $(123)(123) = (132)$
Or $(123)^2 = (132)$;
Also $(123)^3 = I$.
Thus all the elements
May be obtained from (123),
By raising this element
To various powers.
Such a group is called "cyclic".

Further,
If a group is such that
Each letter is changed
Into every other letter
(Including itself)
Once and only once,
It is a "regular" group.
In the above illustration,
This is the case,
Since

Its composition-factors
Are the same numbers
Though perhaps obtained in a
Different sequence.
This important point
Is illustrated
On the inside back cover.

x_1 is changed to x_1 in I,
x_1 is changed to x_2 in (123),
x_1 is changed to x_3 in (132).
Similarly
x_2 is changed to x_2, x_3, x_1
In I, (123), and (132), respectively.
And likewise for x_3.

Hence this group is a
REGULAR CYCLIC GROUP,
Which type of group is essential in
The solution of equations,
As we shall see in a later chapter.

IV. THE GROUP OF AN EQUATION.

Every equation has
A definite group associated with it
For a given field,
As we shall now show.

Suppose we have an equation

$$ax^3 + bx^2 + cx + d = 0$$

Of the third degree,
Having three distinct roots, x_1, x_2, x_3.
And suppose we take some function
Of the roots,
As, for example,

$$x_1x_2 + x_3.$$

If we replace these x's by each other
In this function,
In various ways,
How many such substitutions are possible?

Obviously we can make some substitutions
Of the form (12),
In which only two of the x's
Are interchanged,
Obtaining in this case

$$x_2x_1 + x_3.$$

Similarly the substitution (13)
Would give

$$x_3x_2 + x_1,$$

And so on.

Then there would be
Substitutions of the form (123),
In which three of the x's are interchanged:
Thus (123) applied to the given function

$$x_1x_2 + x_3$$

Would change it to

$$x_2x_3 + x_1,$$

And so on.

If we consider all possible
Replacements of these three x's,
Two at a time and three at a time,
And not forgetting
The Identity substitution
Which replaces
x_1 by x_1, x_2 by x_2, and x_3 by x_3,
There would obviously be
Six possible substitutions in all,
Namely,
I, (12), (13), (23), (123), (132).
That is,
For three x's
There are 3! substitutions[1] possible.

Similarly
If there had been 4 x's,
The number of possible substitutions
Would be 4!
And in general,
For n x's
There would be
n! possible substitutions.
It is important to note that
When a substitution is applied
To a function,
It may or may not
ALTER THE VALUE of the function.
For instance,
The substitution (12)

---

[1] It will be recalled
That the symbol 3! is read
"Three factorial",
And means 3x2x1.
Similarly n! means
$n(n-1)(n-2)\ldots\ldots\ldots 1.$

Applied to the function

$$x_1 + x_2$$

Obviously does NOT alter its value,
But if (12) is applied to

$$x_1 - x_2,$$

It DOES[1] alter it,
Since it changes $x_1 - x_2$ to $x_2 - x_1$.
Now suppose we have
An equation of degree n,
Having n distinct roots,

$$x_1, x_2, x_3, \ldots\ldots\ldots, x_n.$$

It can be shown that
In the function

$$V_1 = m_1x_1 + m_2x_2 + m_3x_3 + \ldots\ldots + m_nx_n$$

(Sometimes called the Galois function)
The m's can be so chosen that
Every possible substitution of the x's
DOES ALTER this function,
And hence
This function can have
n! different values
When the x's are interchanged
In all possible ways.

Representing these n! different values
By $V_1, V_2, V_3, \ldots\ldots\ldots, V_{n!}$,
And forming the expression

$$P(y) \equiv (y - V_1)(y - V_2) \ldots\ldots (y - V_{n!})$$

Where y is a variable,

---

[1] Unless $x_1 - x_2$ happens to equal zero,
Which implies that $x_1 = x_2$,
That is, the roots are not "distinct".
If the roots of an equation $f(x) = 0$
Are not distinct,
We can always get rid of
Such multiple roots by
Dividing the equation through
By the greatest common divisor
Of f(x) and its first derivative.
Hence we need only consider
Equations whose roots ARE distinct.

Consider the following:
If P(y) is multiplied out,
The resulting polynomial in y
May or may not be factorable (reducible)
Depending upon the FIELD
In which the factoring is to be done (see p. 4).

Suppose, for example, that
For a GIVEN FIELD
P(y) is factored so
That the part containing V_1
Which is not further reducible in that field
Is $(y—V_1)(y—V_2)$ or $y^2 —(V_1+V_2)y + V_1V_2$.
Note that in this case
The only V's involved are V_1 and V_2;
Now,
The Identity substitution
And that substitution of the x's
Which changes these V's into each other,
Can be shown to form a group,
And it is this group
That is called
THE GROUP
OF THE GIVEN EQUATION
FOR THE GIVEN FIELD.

Obviously,
The function $y^2—(V_1+V_2)y+V_1V_2$
REMAINS UNCHANGED
By all the substitutions of this group,
Since
Changing V_1 into V_2 and V_2 into V_1,
And the Identity substitution,
Evidently leave this function unaltered.
Similarly
If the irreducible part of P(y)
Had contained besides the V_1,
Also V_2 and V_3,
The group would then consist of
All those substitutions

Which would leave
THIS irreducible part UNALTERED.

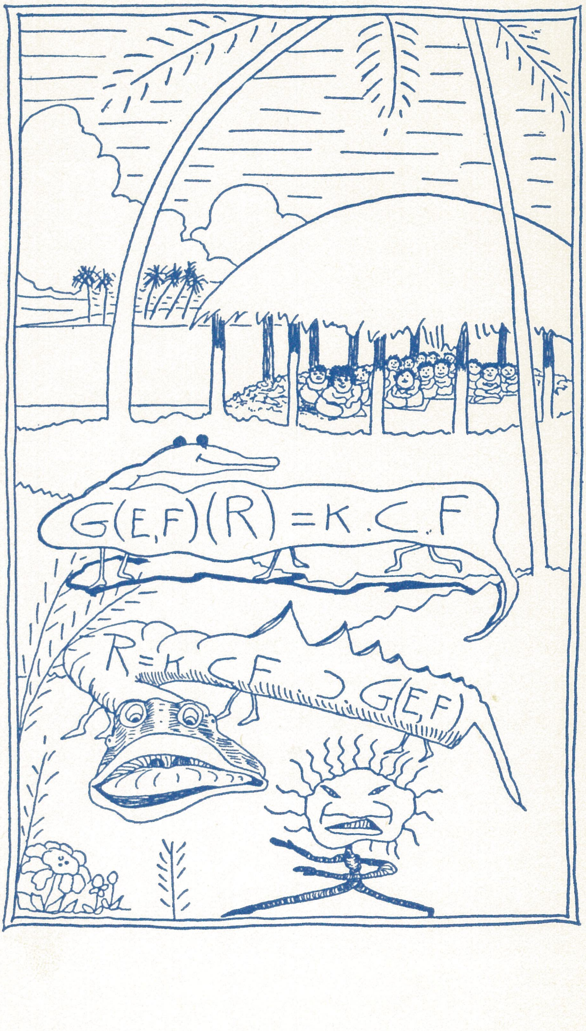
In general, then,
The group of an equation for a given field
Is determined by
That part of $P(y)$ which is
Irreducible in the given field
And contains V_1.
If this irreducible part
Is denoted by $G(y)$,
Then $G(y) = 0$ is called
A Galois resolvent.

It is obvious that
Enlarging the field
MAY make it possible
To continue the factoring further[1],
And hence
Enlarging the field
MAY result
In diminishing the group
Of an equation.
We shall return to
This important point
Later on.

For the general equation of degree n,
$P(y)$ may be completely irreducible
In a field containing the coefficients,
And consequently
Its group contains

---

[1] Thus, in $(x^2 + 1)(x^2 - 3)(x^2 - 1)$,
The part $(x^2 + 1)(x^2 - 3)$ is
Irreducible in the field of
Rational numbers,
But if the field is enlarged
To include all real numbers,
Then the only irreducible part
Is $(x^2 + 1)$.


G(E,F)(R) = K.C.F
R=K.C.F ⊃ G(E,F)

ALL the possible substitutions
On its roots,
Namely, n! substitutions.

Now, FORTUNATELY,
It can be proved that
If the value of ANY function
Of the roots of an equation
Is IN a given FIELD,
Then this function must remain
UNALTERED IN VALUE
By ALL the substitutions
Of the group of this equation
For the given field.[1]
And FURTHERMORE,
If the value of a function
Is NOT in the field,
There must be some substitution in the group
Which DOES alter the value of the function.

I say "fortunately"
Because these important
Characteristic properties
Of the group of an equation
Enable us to find this group
For a given field
Without actually going to the trouble
Of finding a Galois resolvent.

An illustration will make this clear:

Consider the quadratic equation

$$x^2 + 3x + 1 = 0,$$

Having two roots, x_1 and x_2.
Since there are only two roots,
The only possible substitutions

---

[1] For the proof see p. 165 in
L. E. Dickson: Modern Algebraic Theories.
The function must be a rational function
With coefficients in the given field,
And the coefficients of the given equation
Must also be in that field.

Are I and (12).
Therefore the group of this equation
Must contain either both of these
Or I alone,
And that depends upon
The FIELD we choose,
As we shall now see:

Take the function of the roots

$$x_1 - x_2.$$

It is easy to show,
By elementary algebra,
That

$$x_1 - x_2 = \sqrt{b^2 - 4c}$$

For any quadratic of the form

$$x^2 + bx + c = 0.$$

Since in the equation given above

$$b = 3 \text{ and } c = 1,$$

Hence $x_1 - x_2 = \sqrt{5}$.

Now, if the field chosen is
The field of rational numbers,
Then the value of this function
Is NOT in our field,
And therefore
There must be some substitution
In the group
Which DOES alter this function.
Obviously (12) does alter it,
For it changes $x_1 - x_2$ to $x_2 - x_1$.
Consequently
(12) must be in the group,
And the group therefore contains
Both I and (12).

If, on the other hand,
We choose the field of REAL numbers,
Then the value $\sqrt{5}$
IS IN THE FIELD,

And therefore $x_1 - x_2$
Must remain UNALTERED
By ALL the substitutions of the group;
Hence the group cannot contain (12)
Since this substitution alters $x_1 - x_2$.
Consequently,
The group of this equation
For the field of REAL numbers
Contains only I.

Let us take another illustration:
Consider the equation

$$x^3 - 3x + 1 = 0.$$

It has three roots, x_1, x_2, x_3.
The maximum number
Of possible substitutions
Of these three roots
Is SIX:
Namely,

I, (12), (13), (23), (123), (132).

If we choose the field of
RATIONAL numbers,
What is the group of this equation?

Suppose we use the function[1] of the roots

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3).$$

Its value in terms of the coefficients
Is $\pm \sqrt{-4c^3 - 27d^2}$
For a cubic lacking the x^2 term:

$$x^3 + cx + d = 0.$$

---

[1] This type of function
(Namely, the product of the differences
Of all possible pairs of the roots)
Is often very useful in helping
To find the group of an equation.
Other functions are also used,
But it is a comforting thought
That the group of an equation
For a given field
IS UNIQUE
No matter how it has been obtained.

In this particular case

$$c = -3 \text{ and } d = 1,$$

Hence

$$(x_1-x_2)(x_1-x_3)(x_2-x_3) = \pm\sqrt{108-27} = \pm\sqrt{81} = \pm 9.$$

Since $\pm$ 9 is rational
And is therefore in our field,
This function must remain unaltered by
ALL the substitutions of the group.
Now, of the six possible substitutions
Mentioned above,
Only three leave this function unaltered,[1]
Namely, 1, (123), (132).
Hence the group of this particular cubic,
For the rational field,
Contains either these three substitutions,
Or only 1.
Thus the examination of the function

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

Has not yet determined the group exactly.
Let us therefore examine another function,
Namely, the function

$$x_1.$$

If the group contained only 1,
Then the value of this function,
Being unchanged by 1,

---

[1] This should be verified by the reader.
Note that for a particular
Designation of the roots
By x_1, x_2, x_3, respectively,
The value of this function is
EITHER +9 or —9, BUT NOT BOTH:
If it is +9, then it remains +9
Under the three substitutions
1, (123), (132),
But becomes changed to —9
Under the remaining substitutions,
Namely, (12), (13), (23).
And similarly, if its value is —9,
It will remain —9 under 1, (123), (132),
But is changed to +9 under
(12), (13), and (23).

Would have to be in the field.
In other words,
The root x_1 of the cubic
Would be a rational root;
And similarly for x_2 and x_3.

But this cubic HAS NO RATIONAL ROOTS[1].
Hence the group of this cubic,
For the rational field,
Cannot be I alone,
But contains I, (123), and (132).

Thus a consideration of both functions,
$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ and x_1,
Has led to a definite knowledge
Of the group of this equation
For the given field.

This cubic is OF SPECIAL INTEREST
Because it is this equation
Which determines the possibility
Of trisecting an angle, in general,
By means of ruler and compasses only.
We shall study it further in Chapter VI.

The reader may be interested to show
That the group of

$$x^3 - 2 = 0,$$

For the rational field,
Contains SIX substitutions.
This equation obviously represents
The old problem of

---

[1] For, any rational root
Of an equation with integral coefficients,
Whose leading coefficient is 1,
Must be an integer and
A factor of the constant term.
But here the only factors of 1 are ± 1,
Neither of which
Satisfies the equation.

The duplication of the cube.[1]
It will be seen in Chapter VI that
This problem also
Cannot be solved by means of
Ruler and compasses only.

We now see
WHAT IS MEANT BY
The GROUP of an EQUATION for a given FIELD,
And HOW TO FIND IT.

Let us now see
What use we can make of it.

---

[1] That is,
If a unit cube is given,
$x^3 = 2$ represents
A cube whose volume is
Twice the given cube;
The problem is
To find the length of a side x,
By means of
Ruler and compasses only.

V. THE GALOIS CRITERION OF SOLVABILITY.

Galois showed that
An equation is
SOLVABLE BY RADICALS IF AND ONLY IF
ITS GROUP,
FOR A FIELD CONTAINING ITS COEFFICIENTS,
IS A SOLVABLE GROUP.[1]

In Chapter VII we shall show
In some detail
Why it is that
A solvable group makes the equation solvable
With respect to the given field.
For the present let us merely examine
The groups of several equations
For a field containing the coefficients,
And apply the Galois criterion
To determine
Which of them
Are solvable by radicals.

Take first the general quadratic

$$ax^2 + bx + c = 0;$$

Since it has two roots, x_1 and x_2,
Its group, G,
For a field containing its coefficients,
Consists[2] of the substitutions I and (12).
Its only
Maximal invariant proper sub-group
Is obviously I,
Hence its only composition-factor is

$$2/1 = 2.$$

---

[1] In fact this is the reason
For calling the group "solvable" (see p. 23).
[2] See p. 30.

Since this is PRIME,
Then, according to the Galois criterion,
Every quadratic is solvable by radicals.
To be sure this fact was known
Long before Galois,
But it is interesting to see
How simply and elegantly
This conclusion is reached
By means of the Galois theory.

Take next the general cubic
$ax^3 + bx^2 + cx + d = 0.$
Since it has three roots, x_1, x_2, x_3,
Its group, G,
For a field containing its coefficients,
Contains[1] the six substitutions
I, (12), (13), (23), (123), (132),
All the possible substitutions
Of the three roots, x_1, x_2, x_3.
Its only maximal invariant proper sub-group, H,
Contains I, (123), (132);
And the only
Maximal invariant proper sub-group of H
Is I.
Hence the composition-factors are
$6/3 = 2$ and $3/1 = 3$,
Both PRIME numbers.
Therefore, by group theory,
The general cubic also
Is EASILY shown to be
Solvable by radicals.

Next let us consider the
General equation of the fourth degree
$ax^4 + bx^3 + cx^2 + dx + e = 0.$
Its group,
For a field containing its coefficients,
Is of order 4! or 24.
A series of

---

[1] See p. 30.

Maximal invariant proper sub-groups
Contain[1] 12, 4, 2 and 1 substitutions,
Respectively.
Hence the composition-factors are

2, 3, 2 and 2.

Therefore
The general equation of degree four
Is also solvable by radicals,
Since these composition-factors
Are again PRIME numbers.

For the general equation of degree 5,
G contains 5! substitutions,
H contains 5!/2 substitutions,
And the
ONLY[2] INVARIANT PROPER SUB-GROUP OF H
Is I.
Hence the composition-factors are

2 and 5!/2;

Obviously the latter is NOT PRIME,
And therefore
The GENERAL equation of degree FIVE
Is NOT solvable by radicals.

In fact this is true for
The general equation of degree n
For ANY value of n GREATER THAN FOUR[2],
Since the composition-factors are

2 and n!/2,

And the latter is NOT PRIME.

We have thus seen that
The THEORY OF GROUPS
Furnishes an
ELEGANT and POWERFUL METHOD

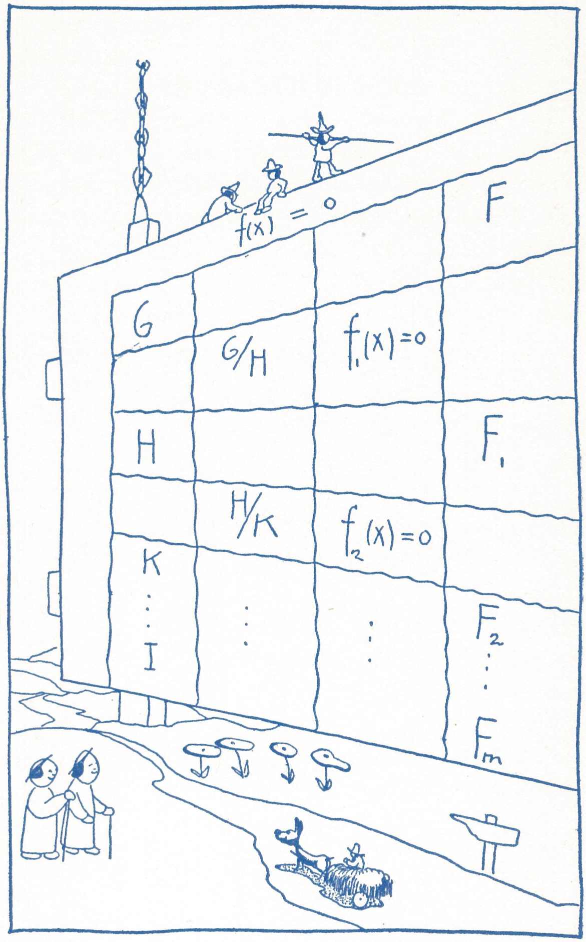
---

1 See Miller, Blichfeldt and Dickson:
Theory and Applications of Finite Groups.

2 For the proof of this
See L. E. Dickson: Modern Algebraic Theories, p. 200,
Theorem 13.

Of determining whether
An algebraic equation is
Solvable by radicals.

Furthermore,
In the next chapter
We shall show
HOW TO SOLVE AN EQUATION
BY GROUP THEORY,
And the bearing that this method has
Upon some old construction problems,
Like that of the trisection of an angle.



f(x) = 0
F
G
G/H
f1(x) = 0
H
F1
H/K
f2(x) = 0
K
I
F2
Fm

VI. CONSTRUCTIONS WITH RULER AND COMPASSES.

Having found a method for determining
Whether an equation is solvable by radicals,
Galois then showed that
An equation which is solvable by radicals
Can be solved by means of a set of
AUXILIARY EQUATIONS,
Whose degrees are the
Composition-factors defined on p. 23.

The following is a sketch of the procedure:
The roots of the FIRST auxiliary equation
Are adjoined to the field, F.
It will be remembered[1] that
Enlarging the field may result in
Increasing the possibilities of factoring P(y)
Thus diminishing the irreducible part[2] of P(y)
And consequently
Decreasing the group of the equation.
Obviously this will happen only
If the enlargement of the field
Is such that
Further factoring of P(y)
Is rendered possible.

Now, in particular,
If the field is enlarged
By the adjoining[3] of the roots
Of the first auxiliary equation,
As mentioned above,

---

[1] See p. 30.

[2] See p. 30.

[3] The reader should clearly understand

Then such further factoring
IS possible,
And the fact is that
The group drops to H[1],
For the new enlarged field, F_1.

If, further,
The roots of the
SECOND auxiliary equation
Are also adjoined,
Then the group drops to K[1],
And so on,
Until
Finally the group becomes I
For the final enlarged field, F_m.
When the group has become I,
It is obvious that
The function x_1,
Being unaltered by
ALL the substitutions in the group,
Namely, by I,
Must be in the field F_m[2].
And similarly for all the other roots.

In this manner,
By examining the group of an equation,

That if, for example,
$\sqrt{2}$ is adjoined to the rational field,
Then the new field will contain
All quantities of the form $a + b\sqrt{2}$,
Where a and b are rational numbers,
But will NOT contain $\sqrt{3}$
Or other irrational numbers.
In other words,
The introduction of $\sqrt{2}$
Does not enlarge the field so as
To become the field of all real numbers.
Thus an enlargement of a field
Usually means the adjoining
Of certain SPECIFIC quantities only.

[1] See p. 23.

[2] See p. 31.

And determining its composition-factors,
We can tell the degrees
Of the auxiliary equations,
And hence we can tell
What sort of quantities
Must be adjoined to the original field
To drop the group to 1;
And thus tell in what field
The roots of the equation exist.

An example will make this clearer:
Take the equation

$$x^3 - 3x + 1 = 0.$$

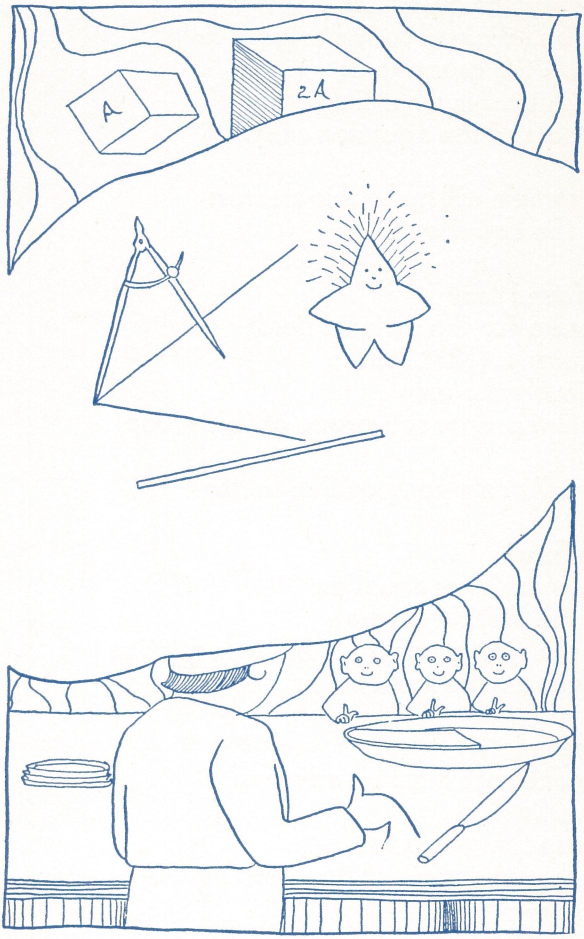
We found that
Its group for the rational field[1]
Contains 1, (123), (132);
Obviously the only
Invariant proper sub-group of this group
Is 1.
Hence its only composition-factor
Is 3.
Therefore
Its only auxiliary equation
Is of the THIRD[2] degree
And the solution of this auxiliary equation
Involves a cube root.

Consequently
This cube root must be adjoined
To the field
To drop the group to 1,
And then the roots of the given equation

---

1 See p. 35.

2 It may seem strange
That the auxiliary equation should be
Of the same degree as the original equation,
BUT, this auxiliary equation
Is of the form $z^3 = g$,
Which is easily solvable.


A
2A

May be obtained in terms of
Quantities in the original field
AND THIS cube root,
By rational operations only.

Let us now see
The connection between this discussion
And the possibility of trisecting an angle
With ruler and compasses only.

In the first place,
What can we do with
Only a ruler and compasses?
Obviously we can only make
Straight lines and circles.
These are represented algebraically
By first and second degree equations,
Respectively.
Hence to get the point of intersection,
We need only solve, at most, a quadratic,
And the coordinates of the solution
Will therefore be expressed
In terms of the coefficients
Combined only by the rational operations
AND a SQUARE root.

That is,
WHATEVER WE CAN DRAW WITH
RULER AND COMPASSES ONLY
CAN BE REPRESENTED ALGEBRAICALLY BY
A FINITE NUMBER OF
ADDITIONS, SUBTRACTIONS, MULTIPLICATIONS, DIVISIONS,
AND SQUARE ROOTS;

Furthermore we know from elementary geometry
That the CONVERSE is also true:
That is, if two lines, a and b,
And the length of the unit,
Are given,
We can construct with ruler and compasses
Their sum, $a + b$, their difference, $a - b$,
Their product, ab, their quotient, a/b,

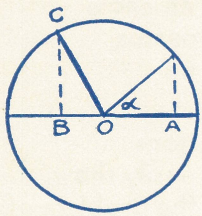
And the square root of any of these
Or of the given quantities,
As, for example, $\sqrt{ab}$ or $\sqrt{b}$
(By the usual mean proportional construction).
And of course
These operations may be
Repeatedly performed upon
Any lines previously obtained.

If we are asked then
Whether a certain construction
Can be done with ruler and compasses only,
We must set up an algebraic equation
That expresses the problem:
If this equation can be factored into
Expressions of the first and second degrees only,
In the given field,
Then all the real roots are obviously constructible
With ruler and compasses;
But even if the equation is
NOT factorable in the way mentioned above,
We MAY still be able to make
The construction with ruler and compasses
PROVIDED THAT
This equation can be solved
SO THAT
The real values of x are expressible
In terms of the given geometric quantities
By means of the rational operations
And square roots,
Applied a finite number of times, only.
If the equation can be so solved,
Then the construction CAN be done
With ruler and compasses,
Otherwise, not.

Let us therefore find an equation
That will represent the problem
Of trisecting an angle.
Obviously if we can show for a

PARTICULAR angle,
That the construction CANNOT be made
With ruler and compasses,
We shall have proved
That an angle cannot, IN GENERAL,
Be so trisected.

Take therefore an angle of 120°:
Suppose it to be drawn
At the center of a circle of unit radius.
Then if we could construct cos 40°,
We would lay off OA equal to cos 40°;



α would then be equal to 40°,
And the required trisection of 120°
Would be accomplished.
Using the trigonometric identity

$$2\cos 3\alpha = 8\cos^3\alpha - 6\cos\alpha,$$

And writing x for $2\cos\alpha$,
We get

$$2\cos 3\alpha = x^3 - 3x.$$

Now, since $3\alpha = 120°$, $\cos 3\alpha = -\frac{1}{2}$;
Hence the equation becomes

$$x^3 - 3x + 1 = 0,$$

The very equation we have been discussing.

If now we are given
ONLY the length of a UNIT,
We can draw the circle shown above,
Then make $OB = 1/2$,
Thus obtaining angle $AOC = 120°$.
Since the only thing given is
The UNIT,
Our field is limited to the

Rational numbers[1].

We now know that
A CUBE ROOT must be adjoined[2]
To the rational field
In order to solve our equation.
BUT
A CUBE root cannot be constructed
With ruler and compasses;

Hence,
We can see that
The solution of the problem
Of the trisection of an angle
With ruler and compasses
Is EASILY shown to be
IMPOSSIBLE.

By similar considerations
The reader can also easily show
That the solution of the problem of
The duplication of the cube
By means of ruler and compasses
Is also impossible.
The equation here is

$$x^3 = 2,$$

And the field is the rational field;
Its group for this field
Contains six substitutions (see p. 35).
Show that both
A SQUARE ROOT AND A CUBE ROOT
Must be added to the field
Before the group drops to 1.
Hence,
Since a cube root cannot be constructed

---

[1] If we start with unity,
We can, by using only the
Four rational operations,
Build up all the rational numbers,
That is, the "rational field".
(See the definition of "field" on p. 4.)

[2] See p. 43.

With ruler and compasses,
This problem cannot be solved by
THESE MEANS.

In like manner,
We can study the problems
Concerning the construction of
Regular polygons of various numbers of sides,
By Group Theory.[1]

---

[1] See Chapter XI. in
L. E. Dickson: Modern Algebraic Theories.

VII. WHY IS THE GALOIS CRITERION TRUE?

We shall now show
Just why it is
That an equation
Is solvable by radicals
If it has a solvable group[1].

Everyone has probably had the experience,
In his early youth,
Of trying to use the relationship
Between the roots and the coefficients
Of an equation,
To solve the equation.
For example,
In the quadratic

$$x^2 + bx + c = 0,$$

Knowing that

$$x_1 + x_2 = -b \qquad (1)$$

And $$x_1 x_2 = c, \qquad (2)$$

Why not solve this pair of equations
For x_1 and x_2?
Of course one quickly discovers that
This method does not work
Because,
If the value of x_1 from (1)
Is substituted in (2),
We get

$$x_2^2 + bx_2 + c = 0,$$

Which is of exactly the same form
As the original quadratic,

---

[1] We shall not prove the converse here;
For that, see p. 198 in
L. E. Dickson: Modern Algebraic Theories.

And hence
This method has only led us back
To the starting point.
But if it were possible to obtain
A pair of equations
BOTH of which are LINEAR,
Then we really COULD[1]
Find the values of x_1 and x_2 from them.

Now,
In the special case
When the group of an equation is a
REGULAR CYCLIC GROUP OF PRIME ORDER,
This can actually be done
As we shall presently see,
And we shall then realize
WHY such an equation
Is SOLVABLE BY RADICALS.
Furthermore,
We shall also see
What bearing this special case has
Upon the more general case of
An equation that has
A SOLVABLE GROUP.

Consider first
The special case of an equation

$$f(x) = 0,$$

Having n distinct roots,
And having a
Regular cyclic group of prime order
For the field[2] determined

---

[1] Provided the determinant of the coefficients is not zero.

[2] Observe that this field,
As well as ANY field whatsoever,
Necessarily contains
ALL THE RATIONAL NUMBERS,
Because
If we take any quantity in a field
(Say, one of the coefficients of the given equation)
And divide it by itself,

By its coefficients
AND the n nth roots of unity.

Let us first recall what is meant by
The n nth roots of unity.
It will be remembered that
The number 1 has
THREE CUBE ROOTS[1]
Namely 1, $-\frac{1}{2}+\frac{1}{2}\sqrt{-3}$, and $-\frac{1}{2}-\frac{1}{2}\sqrt{-3}$,
(Usually denoted by 1, ω, ω^2);
Similarly, in general,
1 has n nth roots,
Which we shall denote by

$$1, \rho, \rho^2, \ldots\ldots, \rho^{n-1}.$$

Further,
These n nth roots involve,
Just as in the case of the
Three cube roots given above,
Only rational numbers and
Roots of rational numbers.
Hence their introduction into the field
In no way affects the statement
That the equation is
"Solvable by radicals".

Now since the group of our equation
Is assumed to be a
Regular cyclic group of prime order,
Its elements are
All the powers of the substitution

$$(123\ldots\ldots n),$$

We get 1,
And from 1, by repeatedly applying
The four rational operations
We get all the rational numbers.
Thus the rational numbers
Are always contained
In EVERY field.

[1] Since $x^3 = 1$ may be written
$x^3 - 1 = 0$ or $(x-1)(x^2+x+1) = 0$,
From which we get the 3 roots given above.

From 1 to n,
The nth power being equal[1] to the Identity.

Let us now take
The set of linear equations

$$x_1 + \rho^k x_2 + \rho^{2k} x_3 + \ldots\ldots + \rho^{(n-1)k} x_n = r_k \quad (3)$$

Where k varies from 0 to n-1.
Observe that this notation
Enables us to write
A whole set of equations
In a single line:
Thus when $k = 0$,
Equation (3) becomes

$$x_1 + x_2 + x_3 + \ldots\ldots + x_n = r_0,$$

For $k = 1$, it becomes

$$x_1 + \rho x_2 + \rho^2 x_3 + \ldots\ldots + \rho^{n-1} x_n = r_1,$$

And so on,
Giving n equations in all.

Now since the sum of the roots
Of any algebraic equation
Is equal to the coefficient of the second term
With the sign changed,
We therefore get the value of r_0
Directly from the given equation.
Let us now see
What kind of quantities
The other r's are:
If we apply the substitution

(123 . . . . . n)

To the left-hand member of equation (3)
It becomes

$$x_2 + \rho^k x_3 + \rho^{2k} x_4 + \ldots\ldots + \rho^{(n-1)k} x_1;$$

But this same result
Might also have been obtained
By multiplying it by ρ^{-k},
Since $\rho^n = 1$.
(ρ being an nth root of unity),
Consequently the substitution

---

[1] See p. 24.

(123 . . . . . n)
Changes the value of r_k to $\rho^{-k}r_k$;
But $(r_k)^n = (\rho^{-k}r_k)^n$ since $\rho^n = 1$.
In other words,
The substitution (123 . . . . . n)
Leaves the value of r_k^n
UNALTERED;
And similarly for
All the other substitutions
Of the group[1] of the given equation.
Therefore $(r_k)^n$,
Being UNALTERED by
ALL the substitutions
Of the group for the given field,
Must have a value which
Is IN this FIELD,[2]
And therefore,
r_k itself may be obtained
By taking the nth root
Of a quantity in the field;
That is to say,
ALL THE r's CAN BE OBTAINED
BY RADICALS
WITH REFERENCE TO THE GIVEN FIELD,
So that the set of equations (3)
Being solvable for the x's
In terms of ρ and the r's,
Is therefore solvable by radicals;
But the x's are the roots

---

[1] Being a cyclic group,
All the elements are powers of (123 . . . . n);
And applying $(123 \ldots n)^2$, for example,
Only means to apply (123 . . . n) twice in succession,
And if applying it the first time
Has produced no change,
Then obviously,
Applying it a second time
Will still leave the value unaltered,
Etc.

[2] See p. 31.

Of the given equation $f(x) = 0$;
We have thus shown that
If the group of an equation
For a given field
Is a
REGULAR CYCLIC GROUP OF PRIME ORDER,
It is
SOLVABLE BY RADICALS.

For example,
In the case of the cubic

$$x^3 - 3x + 1 = 0,$$

We have already seen[1] that
The group of this cubic
For the rational field
Contains I, (123), (132),
And is therefore a
Regular cyclic group of prime order.
We can therefore solve it
By means of the three equations:

$$x_1 + x_2 + x_3 = 0$$
$$x_1 + \omega x_2 + \omega^2 x_3 = r_1$$
$$x_1 + \omega^2 x_2 + \omega x_3 = r_2$$

Where ω is one of the
Imaginary cube roots of unity,
And the values of r_1 and r_2,
As we have seen,
Are obtainable by radicals from
Quantities in the given field.
Or, in other words,
If these radicals are adjoined to the field,
Then the x's exist in this enlarged field.

But what if the group is NOT a
Regular cyclic group of prime order?

For the case of a solvable group
The scheme of solution
Was outlined on page 41.

---

[1] See p. 35.

We saw there that
If the composition-factors are
PRIME,
The equation is still solvable by radicals,
Even though its group is not a
Regular cyclic group of prime order.
This is
BECAUSE IN THAT CASE
EACH AUXILIARY EQUATION
Itself has a group which IS a
Regular cyclic group of prime order
For the field containing
All quantities which have been
Previously adjoined.

Thus,
Since each auxiliary equation has a
Regular cyclic group of prime order,
It is solvable by radicals
AS SHOWN ABOVE,
And consequently,
All the roots of the auxiliary equations
Which have been adjoined
To the original field,
Bring in only radicals of
Quantities which were already in the field.
Hence even in this more general case
The equation is solvable by radicals.

It is interesting to note that the
FIRST auxiliary equation
Can, in general,[1] be:

$$y^2 = (x_1 - x_2)^2 (x_1 - x_3)^2 \ldots (x_{n-1} - x_n)^2,$$

In which the right-hand member
Is the product of the squares
Of the differences
Of all possible pairs of the roots.

---

[1] The first composition-factor
Being, in general, 2 (see p. 39).

This right-hand member
Is equal to the discriminant
Of the equation
When the leading coefficient is 1:
Thus for the quadratic

$$x^2 + bx + c = 0,$$

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4c,$$

Which is the discriminant of this equation.
And similarly,
For equations of higher degrees,
The discriminant can be found
In terms of the coefficients.
The roots of the first auxiliary equation,
Which are merely
The two square roots of the discriminant
Are now adjoined to the given field,
And the group drops to H
For this new field F_1.
The process is now repeated
For the other auxiliary equations.

In the case of the general cubic,
After the roots of the
First auxiliary equation
Have been adjoined to the original field,
The group drops to H;
But H is in this case
A regular cyclic group of prime order,
And consequently
We can at once
Solve the original cubic
By means of the set of equations:

$$x_1 + x_2 + x_3 = -b$$
$$x_1 + \omega x_2 + \omega^2 x_3 = r_1$$
$$x_1 + \omega^2 x_2 + \omega x_3 = r_2$$

Where the r's are obtainable[1]

---

[1] The details are given on p. 136 in
L. E. Dickson: Modern Algebraic Theories,
Where he designates r_1 and r_2 by ϕ and ψ.

By radicals
From quantities in the field
Determined by the coefficients
Of the given cubic AND
The roots of the first auxiliary equation
Which have been adjoined.
Or, in other words,
If the values of these r's
Were also adjoined to the field,
Then the group would drop to I,
Which means that
The x's exist in this final field.
We have thus shown
Why it is that
An equation is solvable by radicals
If it has a solvable group
For the field
Determined by its coefficients
And the n nth roots of unity.
Indeed,
If an equation has a solvable group
FOR ANY FIELD containing the coefficients,
It is solvable by radicals
WITH RESPECT TO THAT FIELD.
We hope that
Enough has been given here
To show that even the details
Are intelligible,
And we trust that the reader
Will continue the study of
This fascinating branch of mathematics,
Particularly since
The use of groups to solve equations
Is by no means the only application
Of the wonderful idea of groups.
In fact,
The use of group theory in geometry[1]

---

[1] See "Projective Geometry"
By Veblen and Young.

Has revolutionized that subject;
Also group theory is fundamental in
The theory of relativity;
Indeed,
As E. T. Bell says[1]:
"Wherever groups disclosed themselves,
Or could be introduced,
Simplicity and harmony
Crystallized out of comparative chaos.
The idea of a group
Was one of the outstanding additions
To the apparatus of scientific thought
Of the last century."

---

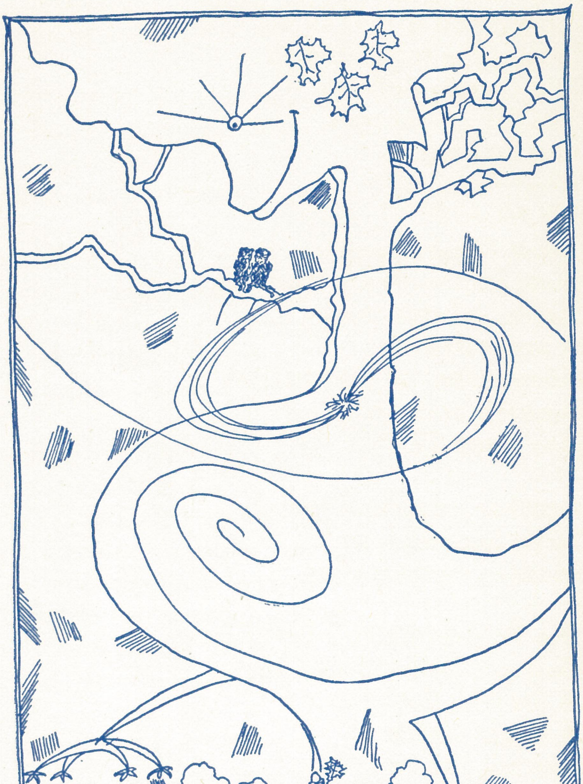
[1] See "The Queen of the Sciences",
By E. T. Bell.
See also the chapter on
The Group Concept
In C. J. Keyser: Mathematical Philosophy.

THE MORAL.

1. Contrary to popular belief
Mathematics is not
A hard set of
Definitions and rules.
By rendering the mind FREE from
Its prejudices and old definitions
Modern mathematics has
Opened up new ground
Of tremendous fertility.
(See pages 14-18).

2. But this freedom is not anarchy—
On the contrary—
Having broadened the definitions
And chosen the postulates and the field,
One must then abide by the
Limitations imposed by these
And remain LOYAL to them
So long as one is working
In this system.
(See pages 3-5).

3. And how shall we determine
What postulates and definitions
And what field
To choose in the first place?
That depends upon the
OBJECTIVE or PURPOSE.
Thus Galois's purpose was
The solution of equations
By certain definite means.
(See pages 1-3).

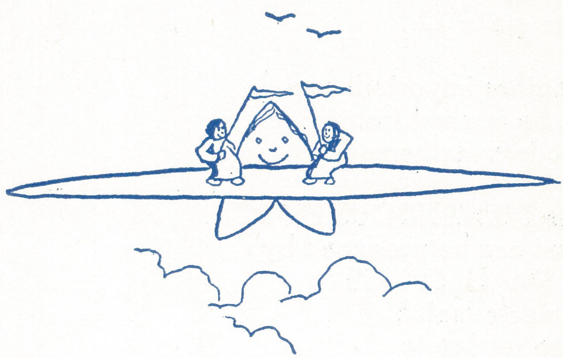


4. Having a purpose,
And having chosen
The postulates in accordance with it,
What is then
THE METHOD?
The method is
To vary the thing studied
By a certain definite
GROUP of changes,
And find out
What remains
INVARIANT
Under these changes.
These invariants are then the
Stable, reliable things
In our system,
Independent of the changes
Imposed upon it.
(See page 22.)

5. Another important moral
To be learned from
Modern mathematics
Is
The TREMENDOUS EFFECT
That can be produced by
A SMALL CAUSE.
A single match
Can set fire to
A whole city.
A problem may be solvable or not
Depending upon some slight change
In the conditions.
(See page 3.)
This is perhaps best illustrated
From geometry,
Where a slight change
In a single postulate,
Leaving all the other postulates the same,

Changed Euclidean Geometry
Into Non-Euclidean![1]

[1] See "Non-Euclidean Geometry or
Three Moons in Mathesis",
In this same series of
Little books.



IMPORTANT TERMS.

hglrl
modern mathematical series

•

(1) non-euclidean geometry or three moons in mathesis (second edition)

(2) galois and the theory of groups

(3) the einstein theory of relativity

(4) others in preparation

drawings by hugh gray lieber
words by lillian r. lieber

* *

price: $1.25 each; 20% discount to teachers and dealers.

copies may be obtained from
H. G. L. R. LIEBER
258 Clinton Avenue, Brooklyn, N. Y.

Consider
the group
containing:
I, (123456), (135)(246), (14)(25)(36), (153)(264), (165432).
The sub-group, H, containing I, (135)(246), (153)(264),
is a MAXIMAL INVARIANT PROPER SUB-GROUP OF G.
And the only maximal invariant proper sub-group of H, is I.
Hence the composition-factors are 2 and 3. But note that the
sub-group I, (14)(25)(36) is ALSO a maximal invariant proper sub-group of G,
Since it is NOT CONTAINED IN A LARGER INVARIANT PROPER
sub-group of G (see p. 24). In this case,
the composition-factors are 3 and 2,
the same numbers as before,
although they were obtained
in the
reverse
order.

A few interesting books:

(1) "Life of Évariste Galois" by M. P. Dupuy: Annales de l'École Normale Supérieure, 1896.

(2) Chapter on Galois' in 'Source Book in Mathematics' edited by David Eugene Smith.

(3) "The Theory of Algebraic Numbers" by L. W. Reid.

(4) "Modern Algebraic Theories" by Leonard Eugene Dickson.

(5) "Ahmes Papyrus" published under the auspices of the Mathematical Ass'n. of America.

(6) "Theory and Applications of Finite Groups" by Miller, Blichfeldt and Dickson.

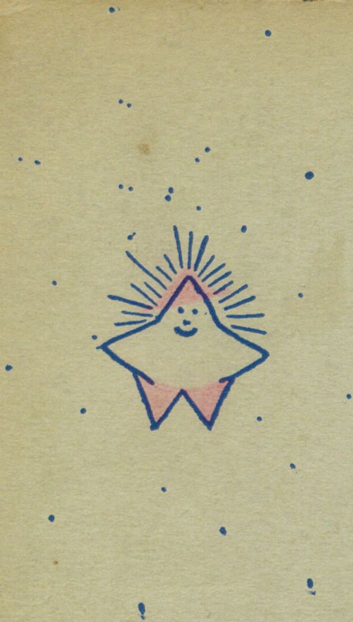
(7) "Elementary Theory of Finite Groups" by L.C. Mathewson.

(8) "Projective Geometry" by Veblen and Young.

(9) "Mathematical Philosophy" by C. J. Keyser.

(10) "The Queen of the Sciences" by E.T. Bell

(11) "Non-Euclidean Geometry" or "Three Moons in Mathesis" by H. G. L. R. Lieber.



a bright star in mathesis